DEPARTMENT OF DEFENSE BLOGGERS ROUNDTABLE WITH COLONEL TONY BUNTYN, U.S. AIR FORCE, VICE COMMANDER, AIR FORCE CYBER COMMAND (PROVISIONAL) VIA TELECONFERENCE TIME: 11:00 A.M. EDT DATE: TUESDAY, JUNE 3, 2008

(Note: Please refer to www.dod.mil for more information.)

CHARLES "JACK" HOLT (chief, New Media Operations, Office of the Assistant Secretary of Defense, Public Affairs): Colonel Tony Buntyn is the vice commander of the Air Force's Air Force Cyber Command (Provisional). And it's the first of its kind among the sister services.

Colonel Buntyn, the floor is yours, if you'd like to make an opening statement for us.

COL. BUNTYN: Okay. Well, thanks very much. I appreciate this opportunity. Part of our mission, in standing up the Provisional Command, is to educate not just the Air Force but the public, on what our mission is. And so again I appreciate this opportunity.

MR. HOLT: All right, sir. Thank you very much. Well, we can move right into questions and answers.

So David, you were first on the line. So why don't you get us started?

Q Hi. It's David with War is Boring.

(Cross talk.)

Can you clarify what Cyber Command's approach will be to new media, things like blogs, social networking?

I understand in the past, the Air Force was concerned that new media were a particular security risk, you know, accessing them from official networks. And it didn't seem that the Air Force was really embracing, you know, Web 2.0 in the way that the other services were.

COL. BUNTYN: David, I'm not sure that I can address how we've embraced Web 2.0, but yeah, it's not so much -- (audio break) -- and blogging. It's, I think, the possibility of visiting certain sites that may have malicious software that would load onto official computers. Just like any other organization, we try to protect our infrastructure and we try to prevent malicious software from being loaded onto the internal network.

Q So, I mean, is a wide blanket ban the best way to do that?

COL. BUNTYN: It may not be the best way to do it, but it is a way.

Q Well, what will be your way?

COL. BUNTYN: Well, right now, I'm a little bit busy doing other things. And that's not my -- you know, I hate to tell you it's not my job, but I'm not responsible at this point for looking at different technology to -- (audio break).

MR. HOLT: All right, it sounds like we're having a little -- excuse me, having some phone dropping out on us here. But as we move along here, Christian?

Q Good morning, General. This is Christian Lowe with military.com. So Air Force Cyber Command works to protect networks and to do cyberdefense and offense for the United States Air Force. But my question is, there are a lot of other military organizations that do this in the other services, as well as, you know, three-letter government agencies that do this kind of thing.

First part of the question is, what is the relationship that you have right now? How is there cross-pollination with these other cyberdefense and offense units or whatever within the U.S. government and the U.S. military, A? And B, who do you see eventually sort of taking the lead in this domain?

COL. BUNTYN: Thanks, Christian. Our relationship is one of cooperation with the three-letter agencies that you mentioned and also the other services. We've -- each one of the services is responsible for the operations and security of their own network (infrastructure ?). And the Air Force Cyber Command -- (audio break) -- and folks, I think if you have the opportunity to mute your phone, that might cut down on some of the additional noise.

MR. HOLT: Okay.

COL. BUNTYN: But we've been training with the -- (audio break) -- DISA, the Joint Task Force Computer Network Operations or Global Network Operations, and also with JFCCNW, for 'net warfare. Those are the two -- (audio break) -- for major combatant command agencies that we deal with. But we also cooperate and share data between the Army and the Navy --

Q Okay.

COL. BUNTYN: -- to help (protect ?) our network. So the -- it's -- if we see an attack of a certain type, it's likely that they've already seen it or they're going to see it.

Q Okay.

COL. BUNTYN: Now, as far as who will take on this role in the future, JFCCNW already has a role, and that's as a component under STRATCOM for 'net warfare. And DISA has the role under the Joint Task Force Global Network Operations, which is also a STRATCOM mission. So I'm assuming that STRATCOM will continue to have this mission.

Q Okay. And have that mission in terms of defense and offense?

COL. BUNTYN: And they currently do, yes.

Q Okay. Okay.

Jack, I'd like to -- I have another question, but if we get to -- if we have more time at the end.

MR. HOLT: Okay. All right. All right. No problem.

And Paul? (Pause.) Paul Crespo, are you still with us? Q No, I was just listening.

MR. HOLT: Okay.

Q I'm good.

MR. HOLT: All right. Okay.

And somebody else joined us on the line. Who's there?

Q This is Ryan Singel from Wired.

MR. HOLT: Okay, Ryan. Go ahead.

Q I'm sorry. Could you maybe explain a little bit more about what the -- what sort of offensive capabilities y'all would like to see in the future and kind of what the problems might be with how that gets targeted, given, you know, that the 'net is not always an easy place to decide, you know, where something is coming from, whether it's foreign, domestic, so forth.

COL. BUNTYN: Ryan, that's a very good point. And I know that I'm not going to be able to talk about -- (audio interference) -- as far as offense -- (audio interference) -- but, you know, general terms. We need -- (audio interference) --

MR. HOLT: Okay, sir, just a second. Somebody's got their phone off of mute. Could you please mute your phone so we can hear? Thank you very much.

Thank you very much.

Go ahead, Colonel. Sorry about that.

COL. BUNTYN: That's all right. And just -- you can use standard terminology in warfare with cyberwarfare. We need the ability to find a target, fix a target so that it's not a mobile target, track, engage -- that's find, fix, track, target, engage. And a target -- what is a target? It could be a logical environment, a logical network. It may be virtual, you know, nodes across multiple networks for, you know, like a command and control system, or it could be physical with a geo- location assigned. But we need the technologies just like we have in kinetic warfare to engage targets when necessary.

MR. HOLT: Okay. And somebody else joined us. Who else is on the line?

Q Yeah, it's Paul McLeary from DTI.

MR. HOLT: Okay, Paul?

Q Speaking about -- and I came late, so you might have already spoken to this. So you're speaking about engaging targets and things like that,

and I was wondering, you know, you find a target and you want to engage it in some way. How do you track them down and what do you exactly mean by engaging target?

COL. BUNTYN: Well, it could be either a kinetic or a non-kinetic effect that you want to achieve. And we need the ability to provide either. It depends on the target. It depends on our rules of engagement. Are we conducting open warfare with an adversary? If that's the case, then we really don't need to get in and be discreet about it. You know, when we drop a JDAM, we leave a big smoking hole. That's not very discreet. But open warfare is not discreet. If we're in that type of a conflict, we need to take out targets one way or another. If it's an IP-based target that is accessible to us and we can take it out electronically, reliably, then that may be the preferred method. But if I can geolocate it, and I need to take it out with a kinetic attack and that is the preferred method and meets the rules of engagement, then that may be the method we choose.

Q Okay. And what are the rules of engagement online or in taking down websites and things like that?

COL. BUNTYN: I am --

Q Are you drawing them up, or is there someone drawing them up now?

COL. BUNTYN: Well, I think rules of engagement are developed for each -- I guess, each conflict. You know, if the commander for Central Command were to draw up the necessary rules of engagement for that particular conflict in that particular AOR -- so I'm certain that JFCCNW has drawn up appropriate rules of engagement for their AOR.

Q Okay.

MR. HOLT: All right. So, okay, anybody else? (Pause.)

Okay, well, let's -- Christian, let's go with the follow-up.

Q Yeah. Thanks, Colonel. Another quick one here. You know, the Air Force does a lot of business with private companies, like Lockheed Martin, Boeing, these types of guys. To what extent are you pressuring them, collaborating with them, asking them politely to secure their own networks against cyberattacks, so that you can defend against an adversary obtaining information about the Air Force through private corporate networks, which may or may not have the same kind of robust defenses that the DOD has and that the Air Force has.

COL. BUNTYN: We do partner with our Defense industrial base companies. But I think it's more of a market incentive for them to protect the data. In many cases, the data that exists on their network is proprietary data, data that they have spent a lot of money doing research and development in producing.

And for that company to retain a competitive advantage, either within the United States or worldwide, they need to protect data. And it's not just Air Force program data that they should be interested in.

Q Okay. So does that mean that you're sort of hands-off about it, then? You're not -- you know, they may want to protect their data, but they may

not have the same kind of technology and access to that technology that the Air Force has in defending its networks.

COL. BUNTYN: A lot of it is not necessarily technology, but information. And we do partner with some of the key defense contractors. And to be honest with you, some of the major defense contractors have some really good technology and know as much or more about this than we do. If you go and look through the chain of companies that attach to some of the big defense companies, down the road they've got -- (audio break) -- security, and they do it very well.

Q Okay. So in other words, you sort of restrict the information -- you said that you collaborate with them on the information. So in other words, you sort of don't give them as much information that you might or something? I don't know what that means.

COL. BUNTYN: No -- (audio break). You know, one thing that we're concerned about is being fair with the defense contractors. And the challenge is protecting the data, and that's up to the company to do that.

Q Okay.

COL. BUNTYN: Companies with -- (audio break). You know, the government can't go in and protect it for them. Okay? Because there's just so many companies. How would we -- if we went in and protected one company, then all companies would expect us to do it. And also, they might see that as providing unfair competitive advantage for one company. It's a very difficult balance that we have to try to achieve.

Q Okay. I understand. Thank you.

MR. HOLT: All right. Anything else? Anybody else? Q Sir, this is David Axe.

COL. BUNTYN: Yes, go ahead.

Q (Audio break) -- terrible today.

MR. HOLT: David, you're breaking up there.

Q I know. I'm -- (audio break).

To follow up on my earlier -- (audio break). Can you hear me?

(Cross talk.)

MR. HOLT: David, you're breaking up really bad.

COL. BUNTYN: Okay. Maybe he'll call back.

MR. HOLT: All right. We'll give him here a second and see if he gets back in. Do we have any other questions out there, while we're waiting for David to come back?

Q I can ask another one, Jack.

MR. HOLT: Okay.

Q Okay, sorry. I have -- this will be my last one, I promise.

Colonel, one other thing, you know, China has been a sort of, you know, the cyberwarfare capabilities of China has been a major storyline recently.

I'm interested in how you view that cyberadversary and whether or not you see potentially a new sort of cyber arms race sparking up against, you know, to protect and to, you know, develop offensive capabilities for and against China.

COL. BUNTYN: No. I'm not going to comment about any specific country. And to do so just really wouldn't be honest. It's --

Q Why would that not be honest?

COL. BUNTYN: Because you know, the entry into this domain, this warfighting domain, is very cheap. A 12-year-old with a laptop can spend a couple hours on the Internet and achieve a pretty good capability, visiting the right website.

We, and I don't think that we're in an arms race. The, and it's not limited to nation states. There are plenty of criminal organizations, that are simply out to make a buck and are using some of the same tools, offensive tools, that a nation state would use.

Q Okay.

And that's even though the latest report on Chinese military power put a big emphasis on China's growing and aggressive cyberwarfare capabilities. That something you're not really keeping an eye on.

COL. BUNTYN: I won't say that we're not keeping an eye on it. I'd just prefer not to comment. Obviously any nation state is interested in what the adversaries are doing.

And I use the term "adversary" because it's generic.

Q Okay.

COL. BUNTYN: Any company or any country or any criminal organization can be your adversary at any time and it depends on their intent, their capability.

Q Okay.

MR. HOLT: And David, did you come back on? Did you get back with us?

Q I am back.

MR. HOLT: Okay.

Q Can you hear me now?

MR. HOLT: Yeah, I got you now.

Q Good Lord. Thanks.

Okay, Colonel, David with War is Boring. So to follow up on my earlier questions, I was really driving at the information warfare aspect of your mission. You know, dealing with cyberthreats seems to have greater information implications than other kinds of warfare. I mean, isn't there a risk with this cyberwarfare that you're going to sort of run roughshod over the Internet's potential for clear and open communication, which, you know, is very much in line with American principles?

COL. BUNTYN: I'm not quite sure that I follow running roughshod over the Internet --

Q Okay, I can -- okay. Look -- I can restate, then. A heightened wariness and -- (inaudible word) -- defenses and offense against cyberthreats might, it seems to me, prevent us from -- prevent the government from using the Internet in the way that, say, private individuals do, to network and communicate and share ideas. What I'm wondering is if a more structured approach to cyberwarfare is going to have a detrimental effect on communication.

COL. BUNTYN: Well, yeah, I don't think it will, anymore than, you know, criminal activity may encourage the police department to close down a street and then public doesn't have access to that street while you have a gunman on the loose and the police are trying to protect the public from harm. If criminal activity or terrorist activity is using a segment of the Internet, we have to target the nodes or the individuals properly. It depends, again, on the rules of engagement and the desired effect.

You know, all the packets across the Internet are attached to or regenerated by a person with an intent. And that's really who you want to get down to. It's the person or the organization that's trying to do you harm. It's not a computer. A computer will only do what people tell it to do. But if a computer is the tool, sometimes we have to take out the tool, because we can't actually reach the person.

Q Colonel, that's -- (inaudible) --

COL. BUNTYN: Let me just also add that, you know, we're -- I think we're in the very early stages of development of computer technology and the Internet and network warfare. But the United States has a history of trying to achieve desired effects with the absolute minimum of collateral damage. And we will use the same principles in network (warfare ?). We will want to understand exactly what the tools that we're using do before we ever try to use them, and we will attempt to minimize any unintended effects.

MR. HOLT: All right.

Q Okay. Thanks.

Q Can I jump in? One last question. Ryan Singel from Wired.com.

MR. HOLT: Okay, yeah.

Q Could you give me a sense of maybe whether there's been kind of a change in -- (inaudible) -- if you start to see -- you know, detect an attempted intrusion or an intrusion into a protected or classified network, and you track it back someplace domestic, what at that point is the -- who investigates at that point? Is that even -- if that investigation done through the Air Force,

or is it in cooperation with, you know, FBI, Secret Service? How are you -- how does that work?

COL. BUNTYN: We partner with the appropriate law enforcement agencies through the Air Force Office of Special Investigations liaison with the FBI or whatever the appropriate agency is for the jurisdiction that's involved.

Q And then what about with an attack from overseas -- (audio break) -- you see somebody from a -- (sitting on a weird ?) server in Russia or in China or, you know, in the Cayman Islands or something? You know, that's been a frustrating thing for the -- for law enforcement to deal with kind of overseas. At one point do you all move from, like, you know, trying to work with, you know, that is purely a criminal investigation to where you actually go and sort of take defensive countermeasures or offensive countermeasures to, you know, attack the server or something like that?

COL. BUNTYN: Well, again, that depends on the rules of engagement. We're always free to take defensive measures --

Q Right.

COL. BUNTYN: -- (protecting ?) our systems. But, you know, it gets kind of old, blocking ports and protocols. And you know that it's -- that's not effective anyway. But certainly we deal with law enforcement to conduct investigations regardless of the location, if it's in a different country, and we work through the law enforcement agencies in various countries.

Q And what is the trigger for deciding something is, you know, a criminal sort of matter that should be investigated and something that, you know, you should be able to, you know, be able to go on offense, you know? It would seem to be very clear if you were being attacked by, say, something you could clearly identify with al Qaeda, you'd clearly be fine with some sort of offensive measure. But when it looks like a, you know, an Eastern European mob that's, you know, that's just trying to get information they can then sell to somebody, how do you -- what's the decision, or, you know, is there kind of -- is there somebody who makes that legal decision on when you can and can't go on offense?

COL. BUNTYN: I'm sorry. I really can't answer that question. It's not that I -- well, it's really that I don't know, okay? (Chuckles.) It's not that I'm trying to avoid it the question, but I just don't know the information. Q Thanks, Colonel.

MR. HOLT: All right, sir.

Well, thank you very much. We're about out of time here. Thank you very much for joining us. Colonel Tony Buntyn is the vice- commander of the Air Force Cyber Command. Thank you, sir, for joining us. We appreciate it, and hopefully we can speak again, sir.

COL. BUNTYN: Well, thank you very much, and I appreciate everyone's time and interest.

MR. HOLT: Thank you, sir.

COL. BUNTYN: Okay.

Q Thanks, Colonel.

END.